**SMLOUVA**

**na dodávku a instalaci monitorovacího systému „Flowmon“**

uzavřená podle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník

## I. Smluvní strany

Organizace: **Centrum pro zjišťování výsledků vzdělávání,** státní příspěvková organizace (CZVV)
Sídlo: Jankovcova 933/63, Holešovice, 170 00 Praha 7
IČO: 72029455
Zastoupené: RNDr. Michaela Kleňhová, ředitelka
Bankovní spojení: Česká národní banka
číslo účtu: [redacted]
(dále jen „objednatel“)

a

Společnost: **NTT Czech Republic s.r.o.**
Sídlo: Milevská 2095/5, Praha 4, Krč, PSČ: 140 00
IČO: 26175738
DIČ: CZ26175738
Zast.: Ing. Petrem Hüblem, jednatelem
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod spisovou značkou C 77064
Bankovní spojení: [redacted]

(dále jen „dodavatel“)

## II. Předmět plnění

1) Předmětem smlouvy je kompletní dodávka, instalace a zprovoznění monitorovacího systému provozu počítačové sítě objednatele, umožňující zejména automatickou detekci bezpečnostních nebo provozních anomálií datové sítě a jejich hlášení formou událostí a to v rozsahu podle technické specifikace a dalších požadavků objednatele, uvedených v příloze č. 1 této smlouvy, která tvoří její nedílnou součást.

2) Předmětem dodávky je i úvodní zaškolení obsluhy, nastavení systému a jeho odladění v prostředí objednatele, nastavení síťových prvků a další související činnosti dodavatele dle požadavků objednatele uvedených v této smlouvě, jejích přílohách a v příslušné zadávací dokumentaci.

3) Smlouvou se dodavatel zavazuje dodat objednateli výše uvedený předmět plnění včas, řádně bez závad a objednatel se zavazuje při dodržení podmínek této smlouvy uvedenou dodávku řádně a včas převzít a zaplatit za ni dohodnutou cenu.

4) Nedodržení technické specifikace požadované objednatelem je vážným porušením této smlouvy a je důvodem k odstoupení od smlouvy.

5) Nesplnění definovaných akceptačních kritérií, je vážným porušením této smlouvy a je důvodem k odstoupení od smlouvy.

6) Dodavatel prohlašuje, že disponuje dostatečným počtem certifikovaných pracovníků. Pro plnění této smlouvy bude použita metodika „Prince2“. Dodavatel prokáže projektového manažera certifikovaného pro tuto metodiku.

7) Veškerý dodaný SW musí být v souladu s legislativou, zejména zákonem č.181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů, a platného nařízení (EU) 2016/679 (GDPR), a musí k němu být dodána v tomto směru i patřičná dokumentace. Před připojením do sítě objednatele musí být provedeny bezpečnostní testy HW i SW na jejich bezpečnost a kompatibilitu v prostředí objednatele. Během testů nesmí dojít k destruktivním zásahům do aplikace či jejích dat.

## III. Doba a místo plnění

1) Doba plnění je sjednána nejpozději do 30 dnů od účinnosti této smlouvy.
2) O úspěšné realizaci dodávky dle článku II. smlouvy bude mezi smluvními stranami sepsán Akceptační protokol.
3) Zodpovědným zástupcem objednatele pro převzetí dodávky dle článku II. této smlouvy je [redacted], [redacted].
4) Prodlení dodavatele s dodávkou delší než 10 pracovních dnů se považuje za podstatné porušení smlouvy a zakládá právo objednatele od smlouvy odstoupit.
5) Místem plnění je sídlo objednatele uvedené v záhlaví této smlouvy.

## IV. Cena plnění

1) Cena za celkovou dodávku v rozsahu dle této smlouvy je oběma smluvními stranami sjednána na základě cenové nabídky dodavatele ve výši:

   **916 215,00 Kč bez DPH (slovy: devět set šestnáct tisíc dvě stě patnáct korun českých)**, tedy 1 108 620,15 Kč včetně DPH v sazbě 21%.
2) Rozpis ceny jednotlivých částí dodávky je uveden v příloze č. 2, která tvoří nedílnou součást této smlouvy.
3) Sjednaná cena je fixní platí až do předání a převzetí celé dodávky.
4) Smluvní cena bude dodavateli uhrazena až po řádném předání a převzetí dodávky Akceptačním protokolem.
5) Zálohy objednatel neposkytuje.

## V. Platební podmínky

1) Dodavatel vystaví fakturu po protokolárním předání a převzetí celé dodávky objednateli, ve které bude samostatně vyúčtována DPH u jednotlivých položek. Přílohou faktury bude kopie dokladu o předání a převzetí – Akceptační protokol.
2) Faktura musí obsahovat náležitosti stanovené zákonem č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů
3) Splatnost faktury se sjednává na 30 dnů od obdržení daňového dokladu objednatelem.
4) Objednatel má právo vrátit dodavateli před termínem splatnosti neproplacenou fakturu k doplnění jako neúplnou, pokud tato nebude obsahovat veškeré náležitosti daňového a účetního dokladu a přílohu, případně další náležitosti dle podmínek této smlouvy a souvisejících právních předpisů. Dodavatel je v tomto případě povinen fakturu bez zbytečného prodlení přepracovat resp. doplnit a doručit ji objednateli.

## VI. Zahájení a ukončení dodávky

1) Dodavatel je povinen elektronicky nebo telefonicky oznámit objednateli nejpozději 3 pracovní dny předem přesné datum a hodinu zahájení prací na dodávce dle této smlouvy.
2) Objednatel převezme plnění v souladu s touto smlouvou a dodavatel předá objednateli také veškerou dokumentaci a doklady, které se k dodávce vztahují.
3) Předávací protokol bude obsahovat kompletní provedení přiloženého akceptačního testu a úplné splnění všech jeho bodů. Nesplnění akceptačních kritérií je vážným porušením smlouvy a je důvodem k odstoupení od smlouvy.

## VII. Záruka za jakost

1) Dodavatel ručí za funkčnost předmětu této smlouvy v rozsahu a parametrech stanovených touto smlouvou a poskytuje záruku v délce 24 měsíců od řádného předání a převzetí plnění dle této smlouvy.
2) Dodavatel se zavazuje po dobu 5 let zajistit příslušnou servisní podporu „Gold Support" zajišťující NBD opravu zařízení a aktualizaci SW po celou dobu platnosti smlouvy.
3) V rámci záruky se dodavatel zavazuje nahlášenou závadu odstranit nejpozději následující pracovní den po nahlášení závady ve výše uvedeném sídle objednatele.

## VIII. Sankce

1) Při prodlení dodavatel s dodávkou, je povinen zaplatit objednateli za každý den tohoto prodlení smluvní pokutu ve výši 1 % ze smluvní ceny dodávky bez DPH.
2) V případě prodlení dodavatele s odstraněním záruční vady je dodavatel povinen zaplatit objednateli za každý den tohoto prodlení smluvní pokutu ve výši 1000,- Kč.
3) V případě prodlení objednatel s úhradou faktury je dodavatel oprávněn uplatnit vůči objednateli zákonný úrok z prodlení.

## IX. Důvěrnost informací

1) Každá ze smluvních stran se zavazuje zachovávat v tajnosti všechny informace důvěrného charakteru, týkající se opačné smluvní strany, které se dozví v průběhu vzájemné spolupráce, a to i po skočení platnosti této smlouvy. Jakékoli tyto informace lze použít jen pro splnění předmětu této smlouvy. Za důvěrné informace se pro účely této smlouvy považují zejména informace obsažené v dokumentaci a materiálech dodaných nebo přijatých v jakékoli formě nebo poskytnuté některou smluvní stranou na základě této smlouvy.
2) Výše uvedené ustanovení a z nich vyplývající závazky se nevztahují na informace:
   - jejichž poskytnutí nebo sdělení bylo předem písemně schváleno chráněnou smluvní stranou,
   - které smluvní strana označila výslovně jako veřejné, které se staly veřejně známými, aniž by smluvní strana povinná zachovávat mlčenlivost porušila povinnosti podle této smlouvy nebo ve smyslu této smlouvy,
   - k jejichž sdělení je smluvní strana povinna podle obecně závazného právního předpisu nebo rozhodnutí soudu, správního či státního orgánu,
   - údaje uvedené v této smlouvě.

## X.
## Závěrečná ustanovení

1) Tato smlouva se řídí právem České republiky, zejména zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
2) Smlouva je uzavřena dnem jejího podepsání oběma smluvními stranami a nabývá účinnosti jejím zveřejněním v registru smluv, jak je níže uvedeno v odstavci 5) tohoto článku smlouvy.

3) Smlouva může být měněna nebo doplňována pouze písemnými, vzestupně číslovanými, dodatky.

4) Dodavatel bere na vědomí, že se realizací této veřejné zakázky stane v souladu s ustanovením § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů nebo veřejné finanční podpory.

5) Tato smlouva bude zveřejněna v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Objednatel zašle tuto smlouvu správci registru smluv k uveřejnění bez zbytečného odkladu, nejpozději však do 30 dnů od uzavření smlouvy. O zveřejnění smlouvy, které podmiňuje její účinnost, bude objednatel neprodleně informovat dodavatele.

6) Smlouva je vyhotovena ve 4 stejnopisech, z nichž každá ze stran obdrží 2 vyhotovení.

7) Nedílnou součásti smlouvy jsou následující přílohy:

   Příloha 1 - Technická specifikace

   Příloha 2 - Rozpis ceny

V Praze dne 21. 11. 2019

za objednatele

…….

RNDr. Michaela Kleňhová
ředitelka

V Praze dne 13. 11. 2019

za dodavatele

…….

Ing. Petr Hübl
jednatel NTT Czech Republic s.r.o.

**Technická specifikace:**
Monitorovací systém musí umožňovat dlouhodobé detailní monitorování veškerého provozu na počítačové síti. Získané statistiky o provozu datové sítě musí umožnit v reálném čase sledovat a vyhodnocovat objemy a strukturu provozu, analyzovat příčiny provozních nebo výkonnostních problémů a odhalovat bezpečnostní hrozby. Je nezbytné, aby monitorovací systém byl zcela nezávislý na použité síťové infrastruktuře a svou funkcí monitorovanou síť neovlivňoval. Ze strany sledované sítě nesmí být monitorovací systém detekovatelný. Systém musí pracovat s technologií datových toků (NetFlow/IPFIX/jFlow/NetStream/cflow).

| Požadavek | Popis |
|---|---|
| **Ucelený, škálovatelný NetFlow/IPFIX monitorovací systém** | Ucelené škálovatelné řešení umožňující dlouhodobé monitorování sítě na bázi technologie datových toků (NetFlow, IPFIX, jFlow, cflow, NetStream). |
| **Podpora infrastruktury** | Podpora IPv4, IPv6, VLAN, MPLS, Ethernet 10Mb/s až 100Gb/s. |
| **Decentralizovaný monitoring lokalit s centrální správou** | Sběr síťových statistik ze vzdálených lokalit s centrálním přístupem k reportům, incidentům a síťovým statistikám a centrální správou systému. |
| **Nezávislost na stávající infrastruktuře** | Nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích (typ nebo výrobce). |
| **Zdroje NetFlow statistik (sondy)** | Specializovaná dedikovaná zařízení (sondy) pro vytváření detailních statistik IP toků o dění na síti, standardizovaný protokol pro výměnu dat o IP tocích (NetFlow v5,v9, IPFIX) |
| **Ukládání statistik a vyhodnocování bezpečnostních hrozeb** | Dlouhodobé ukládání statistik IP toků a jejich centrální sledování a vyhodnocování bezpečnostních hrozeb v síti, prokazování bezpečnostních incidentů. |
| **Zákaznická podpora** | Plná zákaznická podpora v českém jazyce. |
| **Rozhraní pro integraci nástrojů třetích stran** | Otevřené rozhraní a dokumentované API s možností integrace nástrojů i třetích stran. |

## 1. Požadavky na zdroje NetFlow/IPFIX dat (sondy)

Zdoje flow (NetFlow/IPFIX) dat (sondy) jsou výkonné autonomní zařízení, které monitorují síťový provoz, vytváří o něm statistiky v podobě IP toků (NetFlow/IPFIX data) a zasílají tyto statistiky na kolektor pro uložení a další zpracování. NetFlow/IPFIX data obsahují informace o tom, kdo komunikoval s kým, jak dlouho, jakým protokolem, kolik přenesl dat a další informace ze síťové (L3) a transportní (L4) vrstvy OSI modelu. Sondy rovněž umožňují analýzu aplikační vrstvy (L7), identifikaci aplikací (NBAR2) a podrobný monitoring hlavních aplikačních protokolů (např. HTTP, DNS, DHCP). Mimo objemových charakteristik provozu poskytují sondy rovněž výkonové parametry datové sítě (např. RTT, SRT, jitter, retransmise) pro analýzu zpoždění na síti. Díky tomu přináší sonda komplexní přehled a detailní informace o dění v síti a usnadňuje tak řešení síťových problémů, správu a optimalizaci sítě a zvyšuje její bezpečnost.

Sondy jsou nezávislé na použité síťové infrastruktuře a svou funkcí nijak neovlivňují sledovanou síť. K síti jsou připojeny pasivně prostřednictvím SPAN/mirroring portu nebo pomocí TAPu. Ze strany monitorovacích rozhraní připojených do sledované sítě nesmí být zařízení detekovatelné. Sonda je navíc vybavená vlastní kolektorovou aplikací umožňující lokální ukládání a analýzu vlastních NetFlow/IPFIX dat.

| Název požadavku | Popis požadavku |
|---|---|
| **Pasivní zapojení** | Pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAPů, případně v kombinaci se SPAN/mirror porty). |
| **Instalace** | Snadná instalace do stávající síťové infrastruktury – racková montáž nebo šablony pro nasazení virtuálního stroje. |
| **Management rozhraní** | Dva plnohodnotné management (administrativní) porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat. |
| **Zabezpečená vzdálená správa** | Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. |
| **Správa uživatelů a přístupových práv** | Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. |
| **Nastavitelná rychlost monitorovací linky** | Možnost nastavení rychlosti monitorované linky 10/100/1000Mb/s na metalických rozhraních. |
| **Dohled** | Sondu je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP. |
| **Vestavěný kolektor** | Vestavěný kolektor pro dočasné ukládání flow statistik (zajištění redundance), který zahrnuje plnohodnotnou funkcionalitu flow kolektoru. |
| **Časová synchronizace** | Časová synchronizace zařízení proti centrálnímu zdroji času na síti. |
| **Minimální výkon** | Minimální výkon 1 milion paketů za sekundu na každém portu, možnost upgradu na verzi s wire-speed garancí zpracování všech paketů. |
| **Podpora příkazové řádky** | Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky. |
| **Sériová linka pro konfiguraci zařízení** | Možnost přístupu a konfigurace hardwarových zařízení prostřednictvím sériové linky (RS-232). |
| **DNS cache** | Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. |
| **LDAP autentizace** | Podpora autentizace vůči LDAP (Active Directory). |
| **TACACS+ autentizace** | Podpora autentizace vůči TACACS+ |
| **Podpora protokolů pro výměnu dat** | Programové vybavení sondy musí umožnit vytváření NetFlow dat ve formátech verzi 5 a 9, IPFIX. |
| **Podpora spolehlivého a šifrovaného exportu toků dle standardu** | Zařízení umožňuje exportovat statistiky o síťovém provoze (toky) pomocí spolehlivého a zabezpečeného komunikačního kanálu dle standardu RFC 5153. |
| **Zpracování datového provozu** | Zpracování datového provozu IPv4 a IPv6, VLAN, MPLS a jejich reportování na kolektor. |

| | |
|---|---|
| **Analýza tunelovaného provozu** | Monitorování provozu v tunelu (deenkapsulace) GRE, ESP a OTV. |
| **Uživatelsky definované šablony** | Uživatelsky definovatelné šablony pro protokoly NetFlow v9 a IPFIX. |
| **Monitorování MAC adres** | Monitorování a reportování MAC adres ve flow statistikách. Možnost použít MAC adresu jako položku klíče flow záznamu. |
| **Detekce aplikací** | Detekce aplikací dle standardu NBAR2. |
| **Analýza zpoždění na síti** | Reportování RTT, SRT, delay, jitter, retransmise, out-of-order pakety jako součást flow statistik. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| **Monitorování a analýza HTTP provozu** | Monitorování a analýza HTTP provozu - včetně položek typu URL, hostname, stavový kód HTTP, dotazovací metoda. Pro HTTPS reportování hostname jako SNI. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| **Profilování zařízení v síti** | Identifikace operačního systému vč. jeho verze. Identifikace internetového prohlížeče vč. jeho verze. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| **Monitorování VoIP** | Monitorování VoIP statistik, protokol SIP – položky typu SIP URI, jitter, latence, ztrátovost paketů. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| **Monitorování DNS provozu** | Monitorování a analýza DNS provozu - položky jako typ dotazu, dotazovaná doména, návratová hodnota, odpověď. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| **Monitorování SMB/CIFS provozu** | Monitorování a analýza SMB/CISF provozu – položky typu síťová cesta, název souboru, typ operace. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| **Monitorování DHCP provozu** | Monitorování DHCP provozu – položky jako typ DHCP požadavku, originální MAC adresa. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| **Monitorování e-mailového provozu** | Monitorování e-mailového provozu – protokolů SMTP, POP3, IMAP a položek jako uživatelské jméno, jméno odesílatele, selhání autentizace a další. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| **Monitorování MS SQL (TDS protokolu) provozu** | Monitorování Microsoft SQL provozu (TDS protokolu) – položky jako typ dotazu, verze klienta a serveru, uživatelské jméno a další. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). |
| **Monitorování rozšířených L3/L4 informací** | Monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících detekci NATů. |

| | |
|---|---|
| **Kapacita paměti současných toků** | Minimální kapacita paměti současných toků na sondě 500 tisíc toků per monitorovací port. |
| **Nastavení času pro expiraci toků** | Podpora pro nastavení časů u aktivní a neaktivní expirace toků. |
| **Vzorkování** | Podpora vzorkování na úrovni paketů. Podpora vzorkování na úrovni toků. |
| **Simultánní export NetFlow statistik** | Podpora simultánního exportu flow statistik na libovolný počet cílů (redundantní kolektory v různých lokalitách, lokální uložení dat na sondě). Pro různé cíle exportu lze použít různé flow standardy (NetFlow v5, NetFlow v9, IPFIX). |
| **Export na základě filtrování dat na sondě** | Podpora filtrování dat na sondě na základě IP prefixů, VLAN, AS (pro různé cíle exportu různé statistiky). |
| **Vyplňování identifikace AS** | Podpora vyplňování AS na základě vestavěného či dodaného seznamu. |
| **Vyplňování čísla interface** | Podpora pro nastavení hodnoty interface index pro exportované flow statistiky per monitorovací port. |
| **Záchyt provozu v plném rozsahu** | Sonda umožňuje rozšíření o funkcionalitu záznamu provozu v plném rozsahu na základě uživatelem definovaného pravidla záchytu. Rozšíření je řešeno formou licence/instalace SW bez nutnosti změny HW konfigurace. |
| **Podpora vysokorychlostních sítí** | Řešení podporuje sítě s rychlostmi 1/10/40/100GbE (Gigabit Ethernet). |
| **Monitorovací porty sond** | Sondy obsahují až 2x 1GbE monitorovacích portů na zařízení |
| **Výkon sond s 1GbE monitorovacími porty** | Sonda jsou schopna zpracovávat více než 1,8 Mp/s (pakety za sekundu) |

## 2. Požadavky na automatické vyhodnocování NetFlow dat

Systém pro automatické vyhodnocování IP toků umožňuje automatickou detekci bezpečnostních nebo provozních a anomálií datové sítě a jejich hlášení formou událostí. Systém je založen na pokročilých metodách tzv. behaviorální analýzy a umožňuje tak odhalovat hrozby a incidenty, které překonaly zabezpečení na perimetru nebo bezpečnostních ochranu koncových stanic, a pro které dosud není dostupná signatura. Jedná se tak o systém včasné detekce a reakce na bezpečností incidenty, který vhodným způsobem doplňuje stávající nástroje pro předcházení kybernetickým bezpečnostním incidentům. Detekované události je možné dále analyzovat, vizualizovat nebo automaticky reportovat, případně integrovat s dohledovými systémy, incident handling systémy a systémy typu SIEM. Automatická detekce bezpečnostních incidentů, anomálií provozu sítě a konfiguračních problémů výrazně zjednodušuje správu datové sítě, zvyšuje její bezpečnost a umožňuje proaktivně identifikovat příčiny problémů.

| Název požadavku | Popis požadavku |
|---|---|
| **Podpora flow standardů** | Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream. |
| **Deduplikace** | Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou. |

| | |
|---|---|
| **Korelace komunikace před a za proxy** | Systém umožňuje provést korelaci flow statistik před a za proxy serverem před jejich vlastní analýzou s cílem identifikovat provoz procházející proxy serverem a tento provoz přiřadit koncovému uživateli. |
| **Vzorkování na úrovni toků** | Systém podporuje vzorkování na úrovní toků před jejich vlastním zpracováním. |
| **Identita uživatelů** | Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události. |
| **Persistence doménových jmen** | Systém podporuje persistenci doménových jmen, tedy uložení doménové jména původce události v okamžiku zaznamenání výskytu této události. |
| **Detekční pravidla a algoritmy** | Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií. |
| **Detekce síťových útoků** | Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby. |
| **Detekce anomálií v síťovém provozu** | Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace. |
| **Detekce nežádoucích aplikací** | Detekce P2P sítí, a anonymizačních služeb (např. TOR) |
| **Detekce událostí na základě „Threat intelligence“ dat** | Systém umožňuje identifikovat bezpečnostní události (např. komunikaci s botnet command & control centry, přístup na phishing servery, apod.) využíváním zdrojů IP a host reputačních databází poskytovaných výrobcem a aktualizovaných nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci. |
| **Detekce provozních problémů** | Detekce nadměrné zátěže sítě, výpadků služeb, chybějících reverzních DNS záznamů, nových a cizích zařízení připojených k síti. |
| **Detekce síťových anomálií** | Detekce síťových anomálií na základě predikce budoucího chování sítě s využíváním znalosti historie komunikace. |
| **Konfigurační průvodce** | Systém obsahuje konfiguračního průvodce pro nastavení systému při prvním spuštění podle parametrů sítě, do kterého je systém nasazen. |
| **Konfigurace detekčních schopností** | Jednotlivé detekční schopnosti je možné konfigurovat a parametrizovat tak, aby bylo dosaženo maximální efektivity a minimálního počtu falešných poplachů. Detekční mechanismy je možné konfigurovat různým způsobem (např. s různou citlivostí) pro statistiky z různých segmentů sítě (např. LAN nebo DMZ). |
| **Definice vlastních detekčních metod** | Systém umožňuje definovat vlastní detekční metody pomocí poskytnutých příkazů, které vyhledávají ve flow statistikách (včetně informací z aplikační vrstvy) specifické vzory chování. Události detekované vlastními metodami jsou zpracovávány standardně jako události z dostupných detekčních metod (notifikace, reportování, atd.). |

| | |
|---|---|
| **Detekce NATů** | Detekce NATů v síti s využitím rozšířených informací z L3/L4. |
| **Správa filtrů** | Systém umožňuje definovat filtry vč. komplexních filtrů složených z dílčích filtrů. Pro zjednodušení definice filtrů je možné používat operace jako inverze nebo rozdíl filtrů. Filtry je možné exportovat do formátu XML nebo z tohoto formátu importovat. |
| **Správa falešných poplachů** | Případné události, které představují falešné poplachy (false positives) je možné odstranit prostřednictvím jednoduché konfigurace pravidel pro vyloučení falešných poplachů dostupné v uživatelském rozhraní. |
| **Definice závažnosti událostí** | Předdefinované priority událostí s možností uživatelského nastavení závažnosti událostí na základě IP adresních rozsahů, typů událostí, míst výskytu nebo detailů události. Jedna událost může mít v závislosti na konfiguraci přiřazeno více priorit. |
| **Správa uživatelů a přístupových práv** | Správa uživatelů a přístupových práv k událostem prostřednictvím uživatelských rolí. Separace událostí s omezením přístupu pro jednotlivé role/uživatele. |
| **CEF export** | Události je možné automaticky exportovat ve formátu CEF protokolem Syslog. Předpokládané využití této funkcionality je integrace se systémy typu SIEM nebo log management. |
| **SNMP Trap** | Události je možné reportovat do dohledových systémů prostřednictvím funkcionality SNMP trap. |
| **E-mailové notifikace** | Notifikace o detekovaných událostech prostřednictvím e-mailu s podporou různých formátů (HTML, incident handling systém, úsporný textový formát). Možnost připojit vzorek flow dat, na základě kterých byla událost detekována k emailovému reportu. |
| **Záchyt provozu v plném rozsahu** | Na výskytu události je možné automaticky reagovat spuštěním záchytu provozu v plném rozsahu, tedy i komunikaci, která již proběhla a na jejím základu byla detekována anomálie. |
| **Spuštění skriptu** | Na výskyt události je možné automaticky reagovat spuštěním uživatelsky definovaných skriptů. |
| **Uživatelské rozhraní** | Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard (konfigurace per uživatel). Vizualizace průběhu provozu s vyznačením detekovaných událostí v závislosti na nastavené závažnosti událostí. |
| **Integrace informací z jiných služeb** | Systém integruje informace ze služeb DNS, WHOIS, geolokační služby. Uživatelsky definované externí služby fungující na protokolu HTTP. |
| **Kategorie a komentáře** | Události je možné přiřazovat do uživatelsky definovaných kategorií (např. vyřešeno, důležité, apod.). Událostem je možné přímo v systému pořizovat poznámky a komentáře. |
| **Vyhledávání událostí** | Systém nabízí flexibilní uživatelské rozhraní pro vyhledávání událostí dle různých parametrů (typ události, IP adrese původce události, filtr, přiřazení |

| | |
|---|---|
| | události do kategorie, ID události apod.). Události je možné prezentovat různým způsobem (prostý seznam, agregace dle zdrojů, dle cílů apod.). |
| **Interaktivní vizualizace událostí** | Systém umožňuje interaktivní vizualizaci detekovaných událostí formou grafické reprezentace flow statistik, na základě kterých byla událost rozpoznána. |
| **Reporting** | Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF. Automatická distribuce reportů e-mailem. |
| **CSV export** | Události je možné exportovat do formátu CSV pro další zpracování. |
| **Otevřené rozhraní** | Systém detekce anomálií poskytuje dokumentované API pro získávání a zpracování událostí. Prostřednictvím API je možné systém detekce anomálií rovněž konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod, apod.). |

Příloha č. 2 - Rozpis ceny

| PN | Popis | Počet jednotek | Cena za jednotku bez DPH | Celkem bez DPH |
|---|---|---|---|---|
| [redacted] | [redacted] | 1 ks | 144 990,00 Kč | 144 990,00 Kč |
| [redacted] | [redacted] | 1 ks | 236 990,00 Kč | 236 990,00 Kč |
| [redacted] | [redacted] | 5 let | 26 748,00 Kč | 133 740,00 Kč |
| [redacted] | [redacted] | 5 let | 41 499,00 Kč | 207 495,00 Kč |
| [redacted] | Záruční podpora Onsite Parts and Engineer BusHrsxNBD | 2 roky | 15 000,00 Kč | 30 000,00 Kč |
| [redacted] | Instalace | 10 MD | 14 500,00 Kč | 145 000,00 Kč |
| [redacted] | Řízení projektu | 1 MD | 18 000,00 Kč | 18 000,00 Kč |
| **Celkem bez DPH** | | | | **916 215,00 Kč** |
| DPH | | | | 192 405,15 Kč |
| **Celkem s DPH** | | | | **1 108 620,15 Kč** |